IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A data processing device comprising:

an authenticating means for authentication with a device to be authenticated on the basis of key data; and

a key generating means for generating said key data on the basis of the data received from said authenticating means and providing the same to said authenticating means,

wherein said authenticating means provides device identification data identifying the device to be authenticated, master key data, original key data, and service identification data to said key generating means, said service identification data including first service identification data corresponding to a first service to be received by a user of the device to be authenticated and second service identification data corresponding to a second service to be received by the user of the device to be authenticated, said key generating means selects one of said first service identification data or said second service identification data, said key generating means selects a key generation algorithm corresponding to selected service identification data from among a plurality of different key generation algorithms, and said key generating means generates said key data by inputting the device identification data, the master key data, the original key data, and the selected service identification data into ~~using~~ said selected key generation algorithm.

Claim 2 (Original): A data processing device as set forth in claim 1, wherein said key generating means generates said key data unique to the device to be authenticated on the basis of the data received from said authenticating means.

Claim 3 (Previously Presented): A data processing device as set forth in claim 1, wherein said key generating means is provided with a function module having a first input parameter and a second input parameter and generating said key data by using only said first data entered for said first input parameter, and said authenticating means enters said first data for said first input parameter of said function module of said key generating means and enters said second data for said second input parameter.

Claim 4 (Original): A data processing device as set forth in claim 1, wherein said authenticating means provides identification data relating to processing to be performed after said authentication, that is, said first data and said second data received from said device to be authenticated, to said key generating means.

Claim 5 (Previously Presented): A data processing device as set forth in claim 1, wherein said authenticating means provides a function module for performing processing for providing unique data unique to said device to be authenticated received from said device to be authenticated, and said key generating means calls up said function module of said authenticating means and further uses said unique data received from said function module to generate said key data.

Claim 6 (Previously Presented): A data processing device as set forth in claim 5, wherein said authenticating means is realized by executing an authentication program including a function defining said function module by an executing means, and said key generating means is realized by executing a key generation program including a function calling up said function module by said executing means.

Claim 7 (Original): A data processing device as set forth in claim 5, wherein said authenticating means provides said key generating means with said unique data read from a storage means shared between said authenticating means and said key generating means in accordance with execution of said function module when said function module is called up by said key generating means.

Claim 8 (Previously Presented): A data processing device as set forth in claim 1, wherein said data processing device further comprises a key holding means providing a function module for reading out master key data and holding said master key data, and said key generating means calls up said function module of said key holding means and further uses said master key data obtained by said function module to generate said key data.

Claim 9 (Original): A data processing device as set forth in claim 8, wherein said key holding means is realized by execution of a key holding program by an executing means.

Claim 10 (Original): A data processing device as set forth in claim 9, wherein said key holding program is updated independently from programs for realizing said authenticating means and said key generating means.

Claim 11 (Canceled).

Claim 12 (Original): A data processing device as set forth in claim 1, wherein said authenticating means performs authentication with said device to be authenticated on the basis of said key data and, when recognizing mutual legitimacy with said device to be

authenticated, performs processing corresponding to said key data in cooperation with said device to be authenticated.

Claim 13 (Previously Presented): A data processing device as set forth in claim 1, wherein said key generating means generates individual key data unique to said device to be authenticated on the basis of said first data unique to said device to be authenticated, and said authenticating means performs first authentication with said device to be authenticated using fixed key data held by said authenticating means and shared with a plurality of device to be authenticated and performs second authentication with said device to be authenticated using said individual key data generated by said key generating means.

Claim 14 (Original): A data processing device as set forth in claim 13, wherein said authenticating means performs first processing linked with said fixed key data in cooperation with said device to be authenticated after confirming the legitimacy of said device to be authenticated by said first authentication and performs second processing linked with said individual key data in cooperation with said device to be authenticated after confirming the legitimacy of said device to be authenticated by said second authentication.

Claim 15 (Previously Presented): A data processing device as set forth in claim 13, wherein said authenticating means holds original key data linked with said second authentication, and said key generating means generates said individual key data based on unique data received from said device to be authenticated through said authenticating means and said original key data held by said authenticating means.

Claim 16 (Previously Presented): A data processing device as set forth in claim 15, wherein said authenticating means holds identification data of processing to be performed with said device to be authenticated linked with said original key data and provides said key generating means with said original key data linked with said identification data of designated processing, and said key generating means generates said individual key data based on said original key data received by said authenticating means.

Claim 17 (Currently Amended): A data processing method for authentication by an authenticating means with a device to be authenticated on the basis of key data generated by a key generating means, comprising:

receiving from said authenticating means device identification data identifying the device to be authenticated, master key data, original key data, and service identification data at said key generating means, said service identification data including first service identification data corresponding to a first service to be received by a user of the device to be authenticated and second service identification data corresponding to a second service to be received by the user of the device to be authenticated;

generating key data with said key generating means by using only one of said first service identification data or said second service identification data, said generating including selecting a key generation algorithm corresponding to selected service identification data from among a plurality of different key generation algorithms, and said generating including generating said key data by inputting the device identification data, the master key data, the original key data, and the selected service identification data into ~~using~~ said selected key generation algorithm;

providing the key data to said authenticating means; and

authenticating with said authenticating means the device to be authenticated on the basis of said key data received at said providing.

Claim 18 (Previously Presented): A data processing method as set forth in claim 17, wherein in said generating, said key generating means generates said key data unique to said device to be authenticated on the basis of data received from said authenticating means in said receiving.

Claim 19 (Previously Presented): A data processing method as set forth in claim 17, wherein, in said generating, said key generating means generates said key data using only said first data entered for said first input parameter on the basis of a function module having a first input parameter and second input parameter and in said receiving, said authenticating means enters said first data for said first input parameter of said function module of said key generating means and enters said second data for said second input parameter.

Claim 20 (Previously Presented): A data processing method as set forth in claim 17, wherein, in said generating, said key generating means calls up a function module of said authenticating means and further uses unique data unique to said device to be authenticated obtained on the basis of said function module to generate said key data.

Claim 21 (Previously Presented): A data processing method as set forth in claim 17, wherein, in said generating, said key generating means calls up a function module of key holding means and further uses master key data obtained from said function module and held by said key holding means to generate said key data.

Claim 22 (Previously Presented): A data processing method as set forth in claim 21, further comprising:

updating a key holding program for realizing said key holding means independently from a program for realizing said authenticating means and said key generating means.

Claim 23 (Currently Amended): A computer readable medium including computer executable instructions, wherein the instructions, when executed by a processor, cause the processor to perform a method for providing key data to an authentication program performing authentication with a device to be authenticated on the basis of key data and executed in a data processing device, the method comprising:

receiving device identification data identifying the device to be authenticated, master key data, original key data, and service identification data from said authentication program, said service identification data including first service identification data corresponding to a first service to be received by a user of the device to be authenticated and second service identification data corresponding to a second service to be received by the user of the device to be authenticated;

generating said key data by using only one of said first service identification data or said second service identification data, said generating including selecting a key generation algorithm corresponding to selected service identification data from among a plurality of different key generation algorithms, and said generating including generating said key data by inputting the device identification data, the master key data, the original key data, and the selected service identification data into ~~using~~ said selected key generation algorithm; and

providing said key data generated by said generating to said authentication program.

Claim 24 (Previously Presented): The computer readable medium as set forth in claim 23, wherein said generating generates said key data unique to said device to be authenticated on the basis of said first data received at said receiving.

Claim 25 (Previously Presented): The computer readable medium as set forth in claim 23, wherein said method further comprises:

receiving a first input parameter and a second input parameter; and

generating said key data using only said first data entered for said first input parameter, said receiving first data and second data receives said first data and said second data through said first input parameter and said second input parameter of said function, and said generating said key data by using only said first data in said first data and said second data generates said key data using only said first data received through said first input parameter.

Claim 26 (Previously Presented): The computer readable medium as set forth in claim 23, wherein access rights different from said authentication program are defined.

Claim 27 (Currently Amended): A secure application module for communicating with an IC chip storing service date relating to at least one service, comprising:

an authenticating circuit for authentication with a device to be authenticated on the basis of key data; and

a key generating circuit for generating said key data on the basis of the data received from said authenticating circuit and providing the same to said authenticating circuit,

wherein said authenticating circuit provides device identification data identifying the device to be authenticated, master key data, original key data, and service identification data

to said key generating circuit, said service identification data including first service identification data corresponding to a first service to be received by a user of the device to be authenticated and second service identification data corresponding to a second service to be received by the user of the device to be authenticated, said key generating circuit generates said key data by using only one of said first service identification data or said second service identification data, said key generating circuit selects a key generation algorithm corresponding to selected service identification data from among a plurality of different key generation algorithms, and said key generating circuit generates said key data by inputting the device identification data, the master key data, the original key data, and the selected service identification data into ~~using~~ said selected key generation algorithm.

Claim 28 (Currently Amended): A data processing device comprising:

an authenticating unit configured to authenticate a device to be authenticated on the basis of key data; and

a key generating unit configured to generate said key data on the basis of the data received from said authenticating unit and to provide the key data to said authenticating unit,

wherein said authenticating unit is configured to provide device identification data identifying the device to be authenticated, master key data, original key data, and service identification data to said key generating unit, said service identification data including first service identification data corresponding to a first service to be received by a user of the device to be authenticated and second service identification data corresponding to a second service to be received by the user of the device to be authenticated, said key generating unit is configured to generate said key data by using only one of said first service identification data or said second service identification data, said key generating unit is configured to select a key generation algorithm corresponding to selected service identification data from among a

plurality of different key generation algorithms, and said key generating unit is configured to generate a said key data by inputting the device identification data, the master key data, the original key data, and the selected service identification data into ~~using~~ said selected key generation algorithm.

Claim 29 (New): A data processing device as set forth in claim 1, wherein said original key data is unique to the device to be authenticated.

Claim 30 (New): A data processing device as set forth in claim 1, wherein said original key data is identical for a plurality of devices to be authenticated.